Digital Sovereignty in the Post-Soviet Space: A Comparative Analysis of How States Manage External Technology Dependence

1. Introduction

Digital sovereignty is seen as a primary challenge in contemporary international politics. This is because states rely on external technologies, infrastructure, regulatory systems and platforms to ensure digital transformation. Recent research indicates that digital sovereignty is not only limited to state control over the internet but it also includes the capacity of states to shape infrastructure, technological dependencies, rules, and data environments impacting their economic and political autonomy. This links digital sovereignty with other concepts, including data sovereignty, cyber sovereignty, and digital governance. This challenge has become crucial as digital systems now impact economic modernization, geopolitical alignment, public administration, and national security.

To examine this issue, the post-Soviet space offers a professional setting as an example. It is true that these states share several historical legacies considering Soviet institutional development, but they have gone through different economic, geopolitical, and political trajectories since independence. This variation is seen in the digital sphere, where some countries have implemented open and externally-linked governance models, while some have adopted more state-focused or centralized approaches. This is why the region should not be seen as a single technological and political place. It offers a valuable context for investigating how states manage dependence on external technology considering various domestic and international conditions.

This article focuses on Georgia, Armenia, and Kazakhstan. These three examples are very effective. This is because they demonstrate various combinations, reflecting geopolitical orientation, digital modernization strategy, state capacity and regulatory establishment. Armenia, has focused on digital development in a setting shaped by security concerns, structural reliance on external infrastructure, and partners and institutional reform pressures. Kazakhstan in comparison, shows a state-focused and centralized model. Digital modernization, regulatory control and state coordination are seen as important aspects. As far as Georgia is concerned, it focuses on Western-focused reform, openness to external implementation, and digital governance modernization. Differences in these cases make these examples relevant when comparing them in terms of structures.

Major emphasis is laid on this topic because of changing attributes of political transformation and globalization. Digital transition goes beyond technological adoption toward raising questions related to vulnerability, resilience, dependence, control and diversification. States face difficult choices while choosing and depending on foreign platforms, imported infrastructure, regulatory templates, and foreign investment. They also have an opportunity to develop domestic capacity and autonomous governance processes. These choices are very limited for smaller and medium-sized states. This is why digital sovereignty is seen as a crucial matter of managing dependence instead of eliminating it. This is useful in the post-Soviet

region, where both geopolitical pressure and uneven establishment make digital policy political and practical.

The problem lies in how do post-Soviet states manage external technology dependence, and what explains variation considering their approaches toward digital sovereignty? The core objective of this article is to offer a comparative analysis of Georgia, Kazakhstan and Armenia through a mixed-method design including a Digital Sovereignty Index or Technology Dependence Management Score, including comparative analysis of case. The central argument is that digital sovereignty in the post-Soviet space is not only shaped by technological capability but also by institutional strategy, regime type, the extent to which states look for balance openness and geopolitical alignment. When these three countries are examined together, the article contributes to broader comparative politics, political transformation, and digital governance in the post-Soviet space.

2. Literature Review and Conceptual Framework

The literature shows that digital sovereignty has become an important concept in technological, digital governance or state power change. The term explains various forms of autonomy, control and strategic capacity with regards to digital infrastructure, regulatory authority, platforms, standards and data. As per Robles-Carrillo (2023), the language of sovereignty in the digital world is mobilized frequently to indicate claims for autonomy, independence and control over digital infrastructure and technologies. Pohle and Thiel (2020) argue that the concept has now expanded into a policy action that restores the state as a crucial actor in ensuring digital transformation. This is why digital sovereignty is a broader term, referring to both, if states can safeguard themselves online and if they can shape dependencies and institutional factors across the digital system.

One of the primary issues in the literature is that digital sovereignty is linked along with related terms without any sufficient differentiation. One concept is data sovereignty, where the focus changes from the cyberspace as a whole space to the authority to regulate transfer, collection, storage and use of data. Hutchinson et al., (2024) explain data sovereignty as a claim by regions or nations to ensure the flow and management of data in their regions. Data governance is a part of digital sovereignty but digital sovereignty covers various elements, including digital infrastructure, platform regulation, software, procurement choices, cloud dependence, institutional capacity and standards. In simpler words, a state may focus on controlling data while remaining dependent on foreign technical architectures and external vendors and platforms. This is the reason why data sovereignty is treated as one dimension in a digital sovereignty framework. One more term is cyber sovereignty, which refers to a focus on cyberspace, territorial authority and jurisdiction. This cyber aspect is more related to questions regarding state regulation, internet control and jurisdictional authority. Pierucci (2025) sheds light on mapping traditional sovereignty onto cyberspace. He argues that cyberspace does not necessarily fit into territorial models only. Digital sovereignty should not be treated as a synonym for cyber sovereignty.

Additionally, the concept of external technology dependence is also significant. Digital transformation has not decreased dependence but redistributed it in several cases. This is

because states depend on imported hardware, global platforms, foreign cloud providers, cross-border data infrastructure, external software ecosystems, international technical standards, and foreign investment. The literature treats sovereignty not as entirely self-sufficient element but as the capability to manage, diversify, decrease or govern these dependencies. According to Roberts et al., (2021), digital sovereignty action often revolves around safeguarding strategic autonomy, decision-making capability and values with regards to external technological usage. This is important to present in the study as it changes the question away from whether states move forward towards sovereignty or they try to manage dependence in practice.

The concept of digital governance is also linked here but it differs conceptually. OECD material refers digital government as the use of digital technologies to enhance participation, public-sector capacity, trust, policy efficiency and openness. This is not a sovereignty concept but an institutional and administrative concept. Therefore, digital governance concerns how governments organize interoperability, administrative reforms, decision-making, public data systems and service delivery in digital settings. A country may not have high digital sovereignty but might have advanced digital government system if the system relies more on externals standards, foreign infrastructure or external platforms. Also, a state may pursue sovereignty-focused regulation without developing an effective digital governance system. This differentiation matters because the focus is in how states manage external dependence.

The literature also suggests broad strategies through which states react to external technological dependence. The first one is regulation, including platform rules, data protection laws, sectoral digital legislation, cybersecurity frameworks and procurement restrictions (Jiang et al., 2023). Another one is diversification, where states try to not depend on a single external partner, infrastructure provider or platform solely. Another one is control which include direct state coordination, localization measures and centralized oversight along with security filtering. The fourth one is capacity-building like institutional reform, state-led digital infrastructure, digital skills and local ecosystems. In some digital settings, sovereignty is focused through diversification and openness, while in others, through centralization and control. This is the reason why digital sovereignty is treated as a broad spectrum of strategies.

One of the issues in the literature, as explained by Lihua (2024), is the meaning of sovereignty. He proposes that clams are different according to various political environments. Studies have focused on hierarchical control and state authority along with an emphasis on autonomy, democratic values and resilience. Moreover, Roberts et al., (2021) reflect how digital sovereignty is framed around strategic autonomy and protection of public values.

It means the similar sovereignty and language can support various policy logics. Therefore, the digital sovereignty is treated as functional instead of ideological. It indicates how states manage dependence and increase room in a complete digital sphere. The debate is relevant in the post-Soviet space, where states share historical legacies with each other but differ in terms of state capacity, digital policy orientation, institutional development and geopolitical alignment. The literature treats the post-Soviet space not as a single category. Viires (2025) argues that e-government paradox in post-Soviet countries is relevant here. He shows that digitalization in this region is understood as an aspect that reproduce administrative patterns, institutional limits or fragmented accountability. This shows that Soviet legacies do not generate uniform

digital results but digital transformation is filtered through external alignments and political institutions.

This variation is clearly seen in all three cases of Armenia, Georgia and Kazakhstan. According to OECD, Armenia holds robust interest in digital transformation along with regular structural challenges for institutions. The profiling of Georgia revealed digital establishment efforts along with policy coordination. OECD work revealed Kazakhstan points of an ambiguous digitalization category supported by state coordination and continuing framework challenges for business change. These are the differences that reflect those states of the post-Soviet space differ in how they manage technology and external linkages with regards to control and openness. The primary gap lies in the literature around debates that are either too regionally focused or broad. There are useful conceptual tools offered by digital sovereignty scholarships but it is not specific to post-Soviet comparison. Country-specific digital policy reports offer rich material but they do not place all three countries within a mutual framework of external technology reliance management. This article addresses the gap by involving literature on sovereignty and a comparative framework revolving around dependence management. The conceptual logic is that digital sovereignty is understood as a state's capacity to control and manage dependence on external technology with the help of diversification, regulation, strategic control and institutional coordination. On these bases, the article compares how Georgia, Armenia, and Kazakhstan respond to structural pressures through policy and political pathways.

3. Research Design and Methodology

This article uses a comparative mixed-method research design for investigating how post-Soviet states control and manage technology dependence and how it impacts various pathways with regards to digital sovereignty. The design utilizes a structured quantitative comparison with qualitative comparative case analysis and process tracing. This component develops a Digital Sovereignty Management Score (DSMS), which is also called Technology Dependence Management Score. This would compare Georgia, Armenia, and Kazakhstan with a single framework. The research design fits the research question of the article because digital sovereignty is an institutional and political process instead of a measurable technical aspect. The evidence shows that recent digital sovereignty is understood best as a multidimensional aspect linked with strategic capacity, autonomy, dependence management and control instead of self-sufficiency. The article adopts a most-similar systems logic for the selection of Armenia, Georgia and Kazakhstan. This is because they share the historical legacy of Soviet statehood and post-Soviet period. However, they vary according to state capacity, geopolitical orientation, digital governance approaches and regulatory style. They reveal variations in how external technological reliance is managed.

Armenia reflects a smaller state showing institutional reform pressures, structural challenges and security-related challenges while Georgia shows reform-focused and Western-focused model with digital governance openness. Kazakhstan shows a state-led and centralized model, including regulatory coordination and digital advancement. Current reports related to country-focused digital development and post-Soviet government support these states as a uniform category. Digital Sovereignty Management Score focuses on the capacity of a state to manage external dependence, diversify external links, decrease vulnerability and preserve policy-

making. This is how sovereignty is seen as a dependence-management capacity instead of technological independence alone. The score is divided into four dimensions to operationalize the concept, each weighted at 25 percent of the total score. As the article does not claim that one dimension is more vital across all countries so equal weighting is used.

The first dimension is regulatory and institutional capacity, focusing if the state has established the administrative and legal instruments to govern digital reliance. The second one is strategic dependence management, focusing if the state activity diversifies partners, develops national safeguards or regulate important sectors instead of depending on external ecosystems entirely. The third one is domestic digital capability, capturing if the state possesses the human-capital, administrative and infrastructural foundations for decreasing dependence over time. The fourth dimension is operational policy autonomy, focusing on digital governance in practice if it preserves the ability of the state to act with domestic coercion without replacing foreign dependence. The article uses a small set of indicators from official laws, reports and first-party institutional documents across these four dimensions. For regulatory and institutional capacity, indicators include: (1) the existence and quality of personal data protection legislation, (2) the existence of a central digital governance, (3) the existence of a cybersecurity framework and strategy.

For strategic dependence-management dimension, indicators are: (4) evidence of state-focused digital sectors, (5) policy measures for diversification and (6) national strategies to decrease structural vulnerability through security, system-building and procurement. Indicators for domestic capability dimension includes: (7) digital government performance with the UN E-Government Development Index, (8) broader infrastructural and administrative readiness and (9) policy support for business change and digital skills. The dimension of operational autonomy includes: (10) evidence of implementation effectiveness, (11) internet freedom for balancing openness and control and (12) institutional resilience against governance and cyber aspects. Each indicator is scored based on a scale of 0-2; 0 showing that indicator is weak, symbolic or missing; 1 means partial development; and 2 means strong and clearly developed. This keeps the coding transparent by keeping the logic similar across institutional coordination, domestic capacity, cybersecurity, and diversification strategy indicators. In this article, external quantitative data like Freedom on the Net 2024 and UN EGDI 2024 scores are not seen as only measures of sovereignty but as supporting standards within this framework of coding (United Nations Department of Economic and Social Affairs, 2024). For instance, Armenia recorded an EGDI of 0.8422, Kazakhstan 0.9009 and Georgia 0.7792. On the other hand, Freedom House reported internet freedom scores of 72 for Armenia, 37 for Kazakhstan and 70 for Georgia. These scores help in comparison.

The total score is calculated in two stages; first the indicators across four dimensions are averaged and then each dimension contributes up to 25 points, generating a score of 100 in total. The formula is:

$$DSMS_C = \sum_{d=1}^{4} = ((\sum_{i=1}^{nd} s_{cid})/2n_d \times 25))$$

Where, s_{cid} is the score of the country c on the indicator i within the dimension d_1 and n_d is the total number of indicators in that dimension. This means that each dimension is normalized and

prevents a dimension with indicators from dominating the final score. The resulting number does not rank countries in absolute way; it offers a comparative estimate of how each country manages dependency on external technology. A score closer to 100 demonstrates robust strategic and institutional capacity to guide dependence while a score near 0 shows vulnerability and weaker capacity.

The qualitative aspect of the methodology utilizes comparative case analysis along with light process tracing. With the development of quantitative scores, each country is now investigated in determining processes that lead to its position. Three pathways are focused due to qualitative analysis; institutional coordination, state strategy toward openness vs. control. Process tracing is seen in an evidence-based way to determine if a particular policy choices strategic shocks or legal reforms describe pattern in any case. As far as Armenia is concerned, this includes security and reform-related challenges. For Georgia, it includes external standard and reform orientation alignment and for Kazakhstan, it includes robust administrative steering and state-focused coordination. The study has some limitations like some indicators may depend on document-based coding, illustrating interpretive judgment and if number of cases is small, the score is seen as a comparative figure instead of a universal index. Also, official policy commitments do not always show implementation and the article measures dependence management not if this is eliminated.

4. Digital Sovereignty in the Post-Soviet Space: Regional Context

Digital Sovereignty is a vital issue in the post-Soviet space. This is because the region includes a shared historical legacy with uneven technological, political, and economic development. These states have come out from a Soviet institutional environment which organized administrative systems, technological advancement and communications through proper planning. However, after independence, they moved in various directions. Like some pursued open and internationally incorporated reforms while others rebuilt a centralized state control. This is how the region offers a useful and effective setting for investigating how states manage dependence on external technology under various political aspects. Current scholarship on post-Soviet digital change indicates that historical starting points have not generated uniform outcomes of governance, making regional comparison valuable. One core reason why digital sovereignty matters in this region is that digital advancement has been seen under various conditions of structural reliance (Knox & Janenova, 2019). Most of the states (post-Soviet) have not built entirely autonomous digital ecosystems. They depend more on external cloud, imported hardware, outside development support, platform infrastructure and foreign software and transnational standards. The element that makes the post-Soviet space unique is these dependencies interacting with uneven state capacity, weak institutions and changing geopolitical orientations. In this setting, digital policy becomes a question of control, resilience, diversification and the management of vulnerability.

The legacy of Soviet remains important as the region inherited administrative cultures that favor central coordination, state-focused implementation and hierarchy. The governments of post-Soviet also faced pressures related to foreign investment, market reform, cybersecurity threats, global digital incorporation and international regulatory models. This has resulted in an “e-commerce paradox” in the post-Soviet space. This means digital reform can ensure openness

and efficiency but it may also reproduce weaker accountability and limited engagement (International Telecommunication Union, 2021). This is important as it indicates that only digital transformation should not be confused with robust sovereignty. A country may digitalize itself entirely while staying dependent internally. This is why regional variation is important as all three countries have different positions with regards to post-Soviet settings (United Nations Department of Economic and Social Affairs, 2024). Armenia has considered digital transformation as a policy priority but there are structural challenges for companies and institutional integration. OECD has reported the growth in the ICT sector of Armenia while shedding light on barriers for digitalization of businesses, including financing challenges, low awareness and digital skills gaps (OECD, 2024). World Bank also stresses on the significance of Armenia's government approach in adopting digital tools. Georgia shows a different path as its digital establishment has been critically shaped by Western-focused reforms, modernized public administration efforts and open online settings. Georgia is a state having active digital development efforts like policy coordination, governance and infrastructure. Freedom House continues to categorize its internet settings as free even though cyberattacks and online intimidation have been reported. This suggests that Georgia is based on openness, institutional reform and international standards.

In contrast, Kazakhstan shows a centrally-coordinated approach. OECD reports Kazakhstan as a region with detailed digital government system with digital, legal and regulatory conditions for improvement in terms of network affordability, digital improvement and security and digitalization in private-sector (OECD, 2023). Digital transformation has been viewed in terms of private investment, infrastructure quality, resilience and service delivery as per the Resilient Kazakhstan program of the World Bank. The online environment of Kazakhstan, as assessed by Freedom House, shows that it is not free, suggesting higher administrative capability and stronger state coordination, making Kazakhstan vital for digital sovereignty. This regional context shows how important digital sovereignty issue has become in the post-Soviet space. All of the three states are not uniformly integrated or digitally isolated so digital sovereignty emerges through balancing coordination, external reliance, openness and security.

5. Measuring Digital Sovereignty Management

For comparing how Armenia, Georgia and Kazakhstan manage dependence on external technologies, this article interprets a Digital Sovereignty Management Score (DSMS). The objective of this score is not measure the extent to which a state has developed and established the institutional, strategic, operational and regulatory capacity to manage dependence. This calls for digital sovereignty to be understood as the governance of external interdependence under institutional and political conditions. The DSMS has been organized across four dimensions, each weighing 25 percent of the total score.

The first dimension is regulatory and institutional capacity, which identifies if the state has established a legal and administrative framework for digital governance. The second one is strategic dependence management, which determines if the state explores to decrease vulnerability through diversification, resilience and state steering over important sectors. Next one is domestic digital capability, which focuses on administrative, skills-focused and infrastructural foundations required to decrease long-term dependence. The last one is

operational policy autonomy, which captures if digital governance preserves effective space for maneuver instead of depending on formal regulation only. The reason for equal weighting is that there is not assumption of any dimension is more important than the other one in universal settings. Each dimension has three indicators, generating twelve indicators altogether. Regulatory and institutional capacity involves cybersecurity strategy, data protection law and central digital coordination. Strategic dependence management involves state steering of vital sectors, diversification and resilience and the existence of digital transformation strategy. Domestic capability involves e-government performance, business support protocols and digital skills and infrastructure with administrative readiness. Lastly, operational policy autonomy includes openness and control balance, governance and cyber resilience and implementation effectiveness. These indicators have been opted because they can be traced to institutional reports, official laws and national strategies.

Each indicator is coded on an ordinal scale of 0-2, where 0 reflects absent or weak development, 1 shows uneven or partial development and 2 indicates strong and clearly evidenced development. This coding structure is balanced and deliberate. The study includes legal texts, international datasets and documentary evidence, making ordinal approach transparent and defensible. Therefore, the score is intended for comparison instead of making it a universal ranking instrument. It demonstrates structured variation across all cases and offers a baseline for qualitative case analysis. To support indicators, two external benchmarks are integrated into the index. The first is the UN E-Government Development Index (EGDI) 2024, which measures telecommunication infrastructure, human capital and online services. Kazakhstan recorded 0.9009, Armenia 0.8422, and Georgia 0.7792 in the 2204 survey. These values are converted into banded scores for the DSMS; 0.800 and above = 2, 0.650-0.799=1, and below 0.650 = 0. Considering this, Armenia and Kazakhstan receive 2, while Georgia receives 1. Another benchmark is Freedom on the Net 2024, which is used here as a proxy for the control between openness and control in policy autonomy. Armenia scored 72, Georgia 70, and Kazakhstan 37. Now using the banding rule, 70 and above = 2, 40-69 = 1, and below 40 = 0; Georgia and Armenia receive 2, while Kazakhstan receives 0. These measures although do not define digital sovereignty alone but they help in comparison in cross-sectional evidence and information.

Full scoring results are presented below in Table 1.

Table 1: Digital Sovereignty Management Score (DSMS): Armenia, Georgia and Kazakhstan				
Dimension	**Indicator**	**Armenia**	**Georgia**	**Kazakhstan**
Regulatory and institutional capacity	Personal data protection law	2	2	1
	Cybersecurity strategy and implementation framework	1	2	1
	Central digital governance or coordination body	1	2	2
Strategic dependence management	Diversification or resilience policy	1	2	1
	State steering of vital digital sectors	1	1	2
	Digital transformation strategy	2	1	2
Domestic digital capability	E-government performance (EDGI banded)	2	1	2
	Digital skills and business support	1	1	1
	Infrastructure and administrative readiness	1	2	2
Operational policy autonomy	Internet freedom and openness balance	2	2	0
	Implementation effectiveness	1	1	1
	Cyber or governance resilience	1	1	1
	Raw total (out of 24)	16	18	16
	Normalized score (out of 100)	66.7	75.0	66.7

Table 1 shows that the three cases do not only differ in terms of being more or less digitized; they also differ in terms of models of digital sovereignty management. Georgia records the highest score overall because it includes a combination of strong legal and regulatory adaptation, open digital environment and clearer institutional coordination/ The presence of personal data protection law, reform-focused policy trajectory and a cybersecurity strategy supports this result. Armenia lies in the mid-range in terms of score based on a functioning legal framework, open online environment comparatively and reform efforts. However, its overall position is limited due to visible structural challenges and weaker implementation. Both World Bank and OECD report challenges on company-level digitalization skills. Kazakhstan has the same score as Armenia but through a different route. It performs greatly in areas like digital-government capacity, central coordination and state steering. This is consistent with its higher EGDI score and with World Bank and OECD reporting on state-focused digital modernization. However, this benefit is offset by a lower score on the operational and autonomy dimension as the online environment of the country is more restrictive. This comparison is important as it reflects that higher state capacity does not generate a uniform higher digital sovereignty result. Dependence management is strengthened in Kazakhstan's case model through important administrative and control capacity. However, it narrows the openness-based demission considering sovereignty measurement.

This comparative pattern is therefore clear. Georgia approximates an open-integration model, one that pursues sovereignty through openness, external alignment and reform. Armenia demonstrates a reformist yet capacity-constrained model, in which there is presence of legal and policy development along with higher structural vulnerability. Kazakhstan shows a state-coordinated control model, one that places importance on administrative steering to support dependence management but it exists with lower operational openness.

6. Comparative Case Analysis

6.1 Armenia

Armenia demonstrates a case in which digital sovereignty is emphasized through reform-related governance, but under various conditions of structural challenge. Digital transformation has become a core policy priority, as highlighted by international and official assessments. However, the Armenian state still faces a challenge of business digitalization, resilience and administrative coordination. As per OECD reports, the ICT sector in Armenia grew by 20% in 2022. This shows strong interest in digital development, but it also signifies that Armenian SMEs face major hurdles in terms of financial challenges, low digital skills and limited awareness. Similarly, the GovTech assessment by the World Bank proposes that Armenia requires a whole-of-government approach to enable digital tools to support state capacity. This is why Armenia is a useful example as it looks for greater room for maneuver in the entire digital sphere.